Revision Log

Pages Affected	Description of Revision
All	This revision is a total rewrite, no revision bars are used. This revision supersedes all previous Manual E7, Section 5 procedures that are being deactivated in parallel with this revision.

1.0 PURPOSE [S/RID 3]

This procedure defines a standard approach for the control of software and firmware that is not exempt per Manual 1Q, Procedure 20-1, *Software Quality Assurance*.

It further describes the implementation approach of Software Quality Assurance (SQA) activities and actions based on a graded approach driven by the software functional classifications defined in Manual E7, Procedure 2.25, *Functional Classifications* and Manual 1Q, Procedure 20-1.

The software functional classification is based on the intended use of the software and the impact of the results/output on safety, security, and business risk.

2.0 SCOPE

The provisions of this procedure apply only to the Management and Operations (M&O) contractor at the Savannah River Site (SRS) and to subcontractors performing work for the contractor when required by subcontract or applicable law.

This procedure specifically applies when software is developed, procured, maintained, operated, used, or retired.

This procedure shall be used with Manual 1Q, Procedure 20-1, in order to satisfy SQA requirements, per the graded approach.

3.0 DEFINITIONS AND ABBREVIATIONS

General definitions and abbreviations applicable to this procedure are provided in Manual 1Q, Appendix A, *Glossary of Terms*, and Manual E7, Section 6.0, *Glossary*.

4.0 ROLES, RESPONSIBILITIES

NOTE

Refer to Section 5.1.1, Table 1, *SQA Documentation and Responsibility Table*, for common SQA documentation responsibilities. Clarification and additional details may be expanded or restated in the SQA sections.

4.1 Design Authority

NOTE

The Design Authority is assigned by the software owner. The software owner/user is the default Design Authority if no Design Authority is assigned.

The Design Authority is responsible for:

- Complying with the SQA Documentation and Responsibility Table
- Accepting the software for production use

4.1 Design Authority, (cont.)

- Determining if the software should be on the DOE required Safety Software Inventory List (SSIL), per Manual 1Q, Procedure 20-1 by completing the Software Classification process
- Reviewing the functional classification and revising functional classification as needed, if the intended function or effect changes, or if the software is retired
- Reviewing and approving any changes to the software, and data, as required per the configuration control process
- Ensuring required design/technical reviews and Unreviewed Safety Question (USQ)/ Management of Safety Basis (MSB) reviews are conducted in accordance with Manual E7, Procedure 2.60 and Manual 11Q, Procedures 1.05 and 1.07, as appropriate.
- Identifying whether a Facility Operations Safety Committee (FOSC) review is required.

4.2 Design Agency

The Design Agency is responsible for:

- Complying with the SQA Documentation and Responsibility Table
- Functioning as the technical agency
- Developing, reviewing and approving SQA Documentation as required
- Evaluating SQA documentation when software classification changes

4.3 Design Agency Manager

The Design Agency Manager is responsible for:

- Assigning personnel within the Design Agency the responsibility to develop, review, and approve SQA documentation, as required
- Approving a generic Software Quality Assurance Plan (SQAP) that covers multiple software applications that are all supported within that manager’s organization

4.4 Cognizant Quality Function (CQF)

The CQF is responsible for:

- Complying with the SQA Documentation and Responsibility Table
- Reviewing and approving the SQAP and other SQA documents as defined in the SQAP
- Verifying independent reviews have been completed as defined in the SQAP

4.5 Independent Reviewers (IR)

NOTE

The IR may generate documentation for a specific review and submit it to the Design Agency and/or Design Authority.

IR is responsible for:

- Complying with the SQA Documentation and Responsibility Table
- Reviewing SQA documentation for other classifications as defined in the SQAP or as requested by the Design Authority

5.0 REQUIREMENTS

5.1 General

Guide SRNS-IM-2011-00048, *Software Quality Assurance (SQA) Documentation Template Example*, provides supplemental attachments from the E7, Section 5 procedures replaced by this procedure. The guide is available via SRS Site Google search for SRNS-IM-2011-00048.

5.1.1 Engineering Requirements

Peer reviews may be used throughout the SQA process. Peer reviews used as the Independent Reviews are required to be documented.

If Owner responsibilities are required in addition to the Design Authority responsibilities, they shall be defined in the SQAP.

Examples of SQA Documentation are available in the Document Control Register (DCR) and/or in the organization configuration management tool.

Other documents may be used as part of the SQA process or as references to support the SQA process. Examples:

- The facility DSA may be referenced to justify functional classification
- Manual E7, Procedure 2.18, Human Factors Engineering Plan.

Some documents can be provided with a purchased software product. Examples:

- Design Document
- User Manual.

Completed documents shall be maintained in the DCR. Some groups may choose to keep a working copy in their Configuration Management System, as a starting point for revisions.

- If updating a document or plan, verify you have the current approved version and follow the applicable site procedures to update it.

5.1.1 Engineering Requirements, (cont.)

- If developing a new document, you can start with an approved document from another system as a template, compare it to the current Manual 1Q, Procedure 20-1 and Manual E7 requirements for the system classification and create the required documentation.

Support Software (Manual 1Q, Procedure 20-1) includes software tools and system software.

- As appropriate, the software engineering method, software acquisition method, or both shall establish the need for software tools.
- Support software, already approved for and in use at SRS, is incorporated in the SQAP for that system and controlled, as required.
  - Software tools shall be evaluated, reviewed, tested, and accepted for use.
  - Software tools that do not affect the performance of the software need not be placed under configuration control.
  - Changes to the software tool shall be evaluated for impact on the software product to determine the level of reviews and retesting required.
  - System software consists of the computer programs used to provide basic or general system functionality and facilitate the operation and maintenance of the application computer program.
  - Examples include lower level software layers, assemblers, interpreters, diagnostics, and utilities.
  - System software shall be evaluated, reviewed, tested, and accepted for use as part of the software development cycle of a new or revised software product.
  - System software shall be placed under configuration change control.

The following table lists the most common topics, not all inclusive, covered by the SQA process. Some of these topics can be covered in the SQAP document, in a generic SQAP, or as individual or combined documents for the software, based on the graded approach.

5.1.1 Engineering Requirements, (cont.)

Table 1

SQA Documentation and Responsibility Table

Documents or Plans	Design Authority	Design Agency	CQF Quality	IR
Classification (SWCD)	D,A	R	R,A	R,A*
Software Quality Assurance Plan (SQAP)	R,A	D,A	R,A	R,A*
Software List (SIL)	R,A	D,A	R,A*	R,A*
Requirements Specification (RS)	D,R,A***	D,R,A***		R,A*
Design Document (DD)	R,A	D,A		R,A*
Req. Traceability Matrix (RTM)	R,A	D,A		R,A*
Software Test Plan (STP)	R,A	D,A		R,A*
Test Results (TR)	R,A	D,A		R,A*
User's Manual	R,A	D,A		R,A*
Computer Modification Tracker (CMT)	D,R,A***	D,R,A***		
Software Evaluation / Dedication (SEP) and (CGD) Plan (Report)	D,R,A***	D,R,A***	R,A*	R,A*

D = Develops, R = Reviews, A = Approves

**** = If SC/A or SS/B***

******= Design Authority or Design Agency can develop but both shall review and approve.***

5.1.1 Engineering Requirements, (cont.)

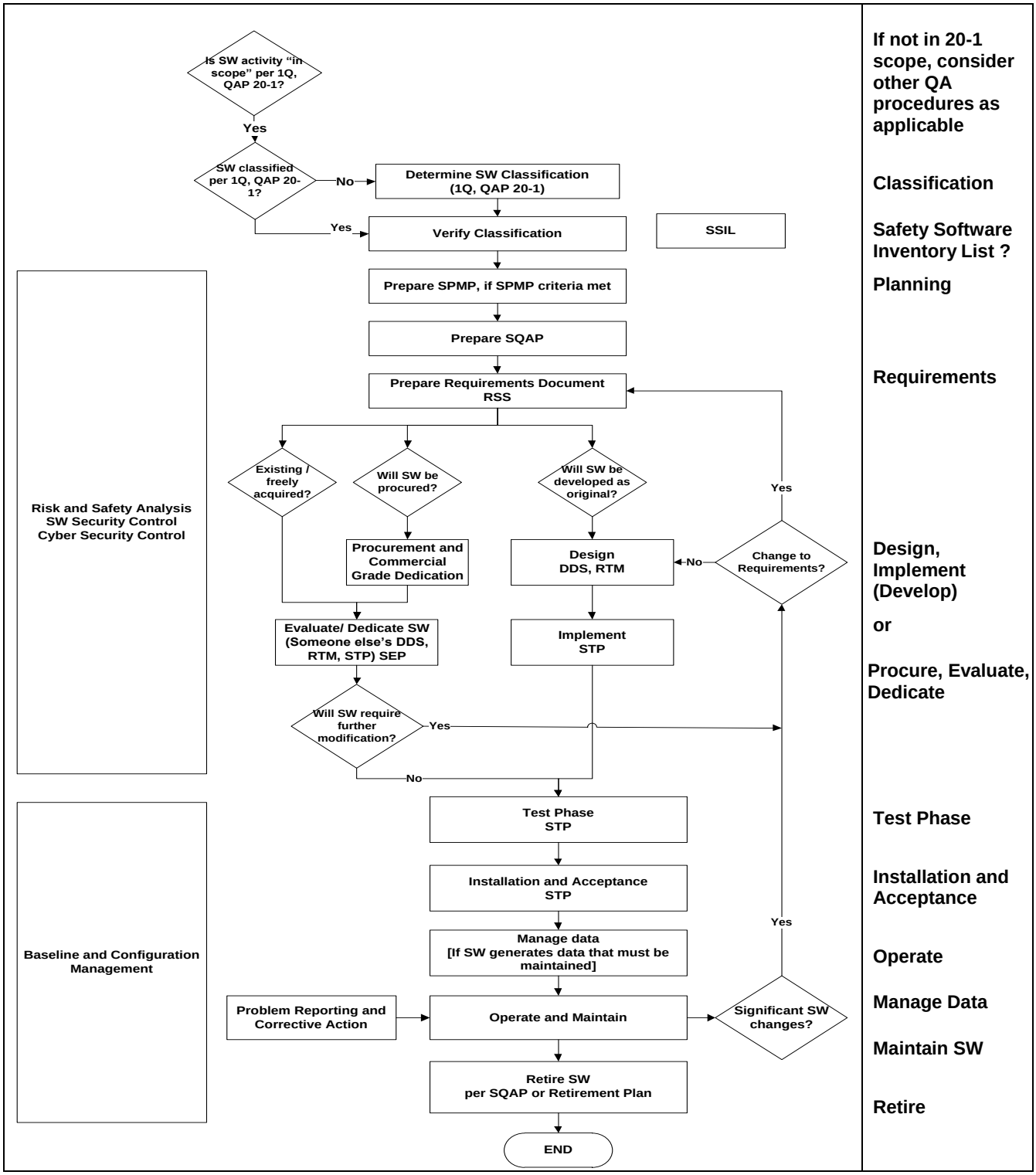
The developer of the document shall obtain a document number and submit it to DCR in accordance with Manual E7, Procedure 1.20, *Engineering Document Numbering System*.

5.1.2 Software Engineering Process

The following flowchart represents the typical software engineering process based on the waterfall software lifecycle model. In some cases the waterfall model from top to bottom is not applicable and the SQA requirements are met using other engineering processes.

The first step in the software engineering process is to determine the classification, so the appropriate rigor and applicable SQA requirements can be determined, before the software is developed, or acquired. Using the graded approach based on classification, all the applicable SQA requirements shall be met before the software is accepted into production.

5.1.2 Engineering SQA Flow (cont.)



5.1.3 Software Matrix Graded Approach

The matrix provided in this Section is from Manual 1Q, Procedure 20-1, Attachment 8.2.

- Lifecycle phases and actions are established and reflected in quality levels using a graded approach.
- The graded approach rigor is applied based on intended use of the software.
- Elements A - J, in the matrix, are defined in Attachment 8.1 (which comes out of DOE Order 414.1C/414-1D).
- This matrix shows the relationship of the SRS Software Quality Assurance (SQA) program to those DOE Order elements.

Developed software is software developed at SRS using the approved SQA program.

Existing software is software in use at SRS that was not developed or acquired using an approved SRS SQA program and once discovered, shall be evaluated. Based on the software classification, as the first step in the evaluation, the SQA rigor is applied to continued use of the software at SRS.

Purchased software is acquired software, using the SRS procurement process and SQA process to acquire and implement the software for use at SRS.

Other Acquired software is software not developed at SRS and not acquired through the site procurement process. This software shall be evaluated and placed under the SRS SQA program as appropriate.

5.1.3 Software Matrix Graded Approach (cont.)

Software Classification Level			SC, A			SS, B			PS, C			GS, D		
DOE O 414.1D Att 4 Sec 4	SQA ACTIVITIES	QAP 20-1	Developed	Existing	Purchased	Developed	Existing	Purchased	Developed	Existing	Purchased	Developed	Existing	Purchased
A, J	Software Classification	5.2	R	R	R	R	R	R	R	R	R	R	R	R
A, J	SQA Procedures/Plans	5.3	R	R	R	R	R	R	R	R	R	R	R	R
A, J	**Life Cycle Phases**	5.4												
E	Requirements	5.4.2	R	R	R	R	R	R	R	G	G	G	G	G
F, G	Design	5.4.3	R	G	G	R	G	G	G	G	G	G	G	G
F	Implementation	5.4.4	R	G	G	R	G	G	G	G	G	G	G	G
H	Testing	5.4.5	R	G	R	R	G	R	G	G	G	G	G	G
H	Installation & Acceptance	5.4.6	R	R	R	R	R	R	R	G	R	G	G	G
H, I	Operations & Maintenance	5.4.7	R	R	R	R	R	R	G	G	G	G	G	G
C	Retirement	5.4.8	R	R	R	R	R	R	G	G	G	G	G	G
A, J	**SQA Actions**	5.5-5.10												
C	Configuration Control	5.5	R	R	R	R	R	R	R	R	R	G	G	G
D	Evaluation	5.6	NA	R	G	NA	R	G	NA	R	G	NA	R	G
D	Procurement Level	5.7.1	NA	NA	1	NA	NA	2	NA	NA	3	NA	NA	3
D	Dedication of Commercial Grade	5.7.2	NA	NA	R	NA	NA	R	NA	NA	G	NA	NA	G
I	Problem Reporting & Corrective Action	5.8	R	R	R	R	R	R	G	G	G	G	G	G
B, G	Risk and Safety Analysis	5.x	R	R	R	R	R	R	G	G	G	G	G	G
B, G	Cyber Security Controls	5.x	CS	CS	CS	CS	CS	CS	CS	CS	CS	CS	CS	CS
A, J	Safety Software Inventory List (SSIL)	5.2 5.10	ALL SOFTWARE THAT MEETS ONE OF THE THREE SSIL DEFINITIONS WILL BE MAINTAINED BY QA											

Definitions:

R	*= Requirement (Shall) must be met and defined in the SQAP.*
G	= A graded approach is used. Consider all requirements, document implemented requirements and justify exceptions.
CS	= Cyber Security requirements per 10Q and 7Q must be met
NA	= Not Applicable

5.2 Software Classification

NOTE

The following procedure Sections (5.2 – 5.10) correspond with Manual 1Q, Procedure 20-1, Sections 5.2 – 5.10.

All software not exempt per Manual 1Q, Procedure 20-1 requires the classification process to be completed.

Software Classification Level			SC, A			SS, B			PS, C			GS, D		
DOE O 414.1D Att 4 Sec 4	SQA ACTIVITIES	QAP 20-1	Developed	Existing	Purchased	Developed	Existing	Purchased	Developed	Existing	Purchased	Developed	Existing	Purchased
A, J	Software Classification	5.2	R	R	R	R	R	R	R	R	R	R	R	R

For required ("R"), all requirements in this section shall be satisfied.

QAP 20-1 Requirements

Refer to Manual 1Q, Procedure 20-1, Section 5.2 for requirements.

Additional Engineering Requirements

Software within an SSC system may have a different classification (lower level) than the system, depending on the impact of the software on the system. This shall be documented.

A system can contain multiple software components and they may have different classifications that are documented and the appropriate level of rigor applied.

A paper OSR 19-337 Software Classification Document (SWCD) document is required for classified software, if the automated process cannot be used due to the presence of classified information.

Support Software already approved for and in use at SRS is incorporated in the SQAP for that system and controlled as required. Support Software (as defined in Section 5.1.1 of this procedure, and Manual 1Q, Procedure 20-1, Section 5.5.6) does not require a separate classification or SQAP.

5.3 SQA Procedures/Plans [S/RID 1, 2, 3]

The SQAP is the governing document for the software engineering process. The SQAP defines the software engineering requirements, the responsible participants, and the required documentation, methods, controls, reviews and approvals for each SQA Activity (SQA Life Cycle Phases and SQA Actions).

Software Classification Level			SC, A			SS, B			PS, C			GS, D		
DOE O 414.1D Att 4 Sec 4	SQA ACTIVITIES	QAP 20-1	Developed	Existing	Purchased	Developed	Existing	Purchased	Developed	Existing	Purchased	Developed	Existing	Purchased
A, J	SQA Procedures/Plans	5.3	R	R	R	R	R	R	R	R	R	R	R	R

For required ("R"), all requirements in this section shall be satisfied.

These procedures/plans may be prepared individually for each software project, or may exist as a generic document to be applied to software prepared within, procured, or used by each organization. If generic plans are used, any unique items for software not covered by the generic plan shall be documented separately.

Examples can be found in DCR (document type code SQP), and industry guidance can be found in IEEE Standard 730, *IEEE Standard for Software Quality Assurance Plans*, and IEEE Standard 730.1, *IEEE Guide for Software Quality Assurance Planning*.

A SQAP can contain some of the required documentation within sections of the SQAP, or be individual documents referenced by the SQAP, or a combination.

QAP 20-1 Requirements

Refer to Manual 1Q, Procedure 20-1, Section 5.3 for requirements.

Additional Engineering Requirements

The SQAP and / or the Software Inventory List (SIL) attached (when a SQAP is used to cover multiple pieces of software) to the SQAP shall identify the following for each software product governed by the SQAP, in addition to what is in Manual 1Q, Procedure 20-1:

- Planned software engineering approach
- Any deviation from SQA requirements shall be documented and justified
- Include Support software (software tools and system software) that can affect the performance of the primary software product(s), as appropriate.

5.3 SQA Procedures/Plans [S/RID 1, 2, 3], (cont.)

Additional Engineering Requirements (cont.)

The Design Agency Manager can approve a generic SQAP that covers multiple software applications that are all supported within that manager's organization.

A Software Project Management Plan (SPMP) may be developed, if required by the Design Authority. Examples of an SPMP can be found in DCR (document type code SMP) and industry guidance in IEEE Standard 1058, *Software Project Management Plans*.

See the SQA Documentation and Responsibility Table in Section 5.1.1 of this procedure for responsibilities. The Design Authority and Design Agency may document other applicable SQA responsibilities in the SQAP.

5.4 Software Engineering Life Cycle [S/RID 1, 2]

5.4.1 Introduction

This procedure defines the implementation requirements and responsibilities for a standard approach for the quality control of software and shall be used with Manual 1Q, Procedure 20-1. Software shall be controlled throughout its life cycle, using a graded approach, based on its software classification and as documented in the SQAP.

QAP 20-1 Requirements

Refer to Manual 1Q, Procedure 20-1, Section 5.4.1 for requirements.

SQA Action: Risk and Safety Analysis

Risk and safety analysis requirements are determined starting with the software classification level.

Software Classification Level			SC, A			SS, B			PS, C			GS, D		
DOE O 414.1D Att 4 Sec 4	SQA ACTIVITIES	QAP 20-1	Developed	Existing	Purchased	Developed	Existing	Purchased	Developed	Existing	Purchased	Developed	Existing	Purchased
B, G	Risk and Safety Analysis	5.x	R	R	R	R	R	R	G	G	G	G	G	G

For required ("R"), all requirements in this section shall be satisfied. If graded ("G"), consider all requirements, and document implemented requirements.

The SQA work processes and project activities are established to balance safety with acceptable levels of risk; this is documented throughout the SQA process. The first step is the classification based on safety, security, and business risk.

Refer to Manual 1Q, Procedure 20-1, Section 5.4.1, Item 3 for requirements.

5.4.2 SQA Life Cycle: Requirements Phase

Software requirements define the functionality, performance, design constraints, attributes, and external interfaces necessary to design or acquire software.

- The requirements also define the response of the software to anticipated inputs.
- The requirements shall be traceable throughout the software.

Software Classification Level			SC, A			SS, B			PS, C			GS, D		
DOE O 414.1D Att 4 Sec 4	SQA ACTIVITIES	QAP 20-1	Developed	Existing	Purchased	Developed	Existing	Purchased	Developed	Existing	Purchased	Developed	Existing	Purchased
A, J	Life Cycle Phases	5.4												
E	Requirements	5.4.2	R	R	R	R	R	R	R	G	G	G	G	G

For required ("R"), all requirements in this section shall be satisfied. If graded ("G"), consider all requirements, and document implemented requirements.

QAP 20-1 Requirements

Refer to Manual 1Q, Procedure 20-1, Section 5.4.2 for requirements.

Additional Engineering Requirements

The Requirements Specification (RS) can be a section within the SQAP or a separate document.

Examples can be found in DCR (document type code RS), and industry guidance can be found in IEEE Standard 830, *IEEE Recommended Practice for Software Requirements Specifications*. IEEE Standard 1233, *IEEE Guide for Developing System Requirements Specifications*, may be used for additional guidance.

The Design Authority is responsible for preparing and issuing an original or revised RS. The Design Authority can delegate the development of the RS, but the Design Authority shall review and approve.

If the software classification is SC/A or SS/B, or at the discretion of the Design Authority, the requirements shall include support of manual or automatic self-check diagnostics to detect computer hardware or system failures.

Specific details of requirements (e.g. temperature constants) that cannot fully be defined in the initial RS shall be indicated as TBD (To Be Determined) and completed when the information is available. However, all "TBDs" shall be resolved (either replaced by an approved requirement or deleted) before final software acceptance testing can be completed.

5.4.2 SQA Life Cycle: Requirements Phase (cont.)

Additional Engineering Requirements, (cont.)

If the RS or equivalent requirements document includes human-system (user) interface requirements for a process control system, refer to Manual E7, Procedure 2.18, to select applicable requirements.

Identify non-critical as well as critical requirements. A critical requirement is one that shall be satisfied in order for the software to be accepted.

- Critical requirements can be used as the Critical Characteristics for Acceptance requirements for the Commercial Grade Dedication (CGD) process, when CGD is required.
- Once identified, the critical and non-critical requirements can then be prioritized for implementation.

Refer to the SQA Documentation and Responsibility Table in Section 5.1.1 of this procedure for responsibilities. The Design Authority and Design Agency may document other applicable SQA responsibilities in the SQAP.

5.4.3 SQA Life Cycle: Design Phase [S/RID 2]

The Design lifecycle phase describes how the design of the software product shall be addressed.

- Include in the description how the classification-dependent requirements below shall be accomplished during the design phase.
- If required, the Design Document (DD) for Software (known as DDS Design Document for Software to some) and the Requirements Traceability Matrix (RTM) are started by the end of the Design Phase.

Software Classification Level			SC, A			SS, B			PS, C			GS, D		
DOE O 414.1D Att 4 Sec 4	SQA ACTIVITIES	QAP 20-1	Developed	Existing	Purchased	Developed	Existing	Purchased	Developed	Existing	Purchased	Developed	Existing	Purchased
A, J	Life Cycle Phases	5.4												
F, G	Design	5.4.3	R	G	G	R	G	G	G	G	G	G	G	G

For required ("R"), all requirements in this section shall be satisfied. If graded ("G"), consider all requirements, and document implemented requirements.

5.4.3 SQA Life Cycle: Design Phase [S/RID 2] (cont.)

QAP 20-1 Requirements

Refer to Manual 1Q, Procedure 20-1, Section 5.4.3 for requirements.

Additional Engineering Requirements

The DD can be a section within the SQAP, a separate document or combined with other SQA documents.

Examples can be found in DCR (document type code DD), and industry guidance can be found in IEEE Standard 1016.1, *IEEE Guide to Software Design Descriptions.* IEEE Standard 1016, *IEEE Recommended Practice for Software Design Descriptions*, may be used for additional guidance.

For developed software classified as SC/A or SS/B, an RTM is required. For another classification, apply a graded approach.

If the software being designed requires an RTM, the following items shall be included in addition to what is in Manual 1Q, Procedure 20-1.

- Map the requirement(s) implemented in the design
- Test case reference linking a test case to its corresponding requirement.

The RTM shall be a document that is updated through the completion of the acceptance of the software into production. Examples can be found in DCR (document type code RTM).

If requirements in the RS need to be modified, then those requirements and the updated RS shall be reviewed and approved as required.

If modifications made to the RS lead to changes in the DD, RTM and/or test cases, then the Design Agency shall update the DD, RTM, and/or test cases. Same approvals as original are required.

As required and specified by the SQAP, design review(s) are performed at a frequency agreed upon by the Design Authority and Design Agency.

Software shall be reviewed in accordance with Manual E7, Procedure 2.60, *Technical Reviews*, as well as any additional review requirements specified in the SQAP.

Refer to the SQA Documentation and Responsibility Table in Section 5.1.1 of this procedure for responsibilities. The Design Authority and Design Agency may document other applicable SQA responsibilities in the SQAP.

5.4.4 SQA Life Cycle: Implementation Phase (Developing the Code and Testing Approach) [S/RID 2]

Describe how the implementation of the software product shall be addressed. Include in the description how the requirements below shall be accomplished during the implementation lifecycle activity.

Software Classification Level			SC, A			SS, B			PS, C			GS, D		
DOE O 414.1D Att 4 Sec 4	SQA ACTIVITIES	QAP 20-1	Developed	Existing	Purchased	Developed	Existing	Purchased	Developed	Existing	Purchased	Developed	Existing	Purchased
A, J	Life Cycle Phases	5.4												
F	Implementation	5.4.4	R	G	G	R	G	G	G	G	G	G	G	G

For required ("R"), all requirements in this section shall be satisfied. If graded ("G"), consider all requirements, and document implemented requirements.

QAP 20-1 Requirements

Refer to Manual 1Q, Procedure 20-1, Section 5.4.4 for requirements.

Additional Engineering Requirements

Modifications to baseline deliverables are performed in accordance with the requirements in the SQAP.

Design and implementation modifications are performed by the Design Agency or as outlined in the SQAP.

Refer to the SQA Documentation and Responsibility Table in Section 5.1.1 of this procedure for responsibilities. The Design Authority and Design Agency may document other applicable SQA responsibilities in the SQAP.

5.4.5 SQA Life Cycle: Test Phase (Verification) [S/RID 2]

The Test Phase describes how the testing of the software product shall be addressed. This includes in the description how the classification-dependent requirements below shall be accomplished during the test lifecycle activity.

Software Classification Level			SC, A			SS, B			PS, C			GS, D		
DOE O 414.1D Att 4 Sec 4	SQA ACTIVITIES	QAP 20-1	Developed	Existing	Purchased	Developed	Existing	Purchased	Developed	Existing	Purchased	Developed	Existing	Purchased
A, J	Life Cycle Phases	5.4												
H	Testing	5.4.5	R	G	R	R	G	R	G	G	G	G	G	G

For required ("R"), all requirements in this section shall be satisfied. If graded ("G"), consider all requirements, and document implemented requirements.

5.4.5 SQA Life Cycle: Test Phase (Verification) [S/RID 2], (cont.)

QAP 20-1 Requirements

Refer to Manual 1Q, Procedure 20-1, Section 5.4.5 for requirements.

Additional Engineering Requirements

Testing of non-critical requirements shall be at the discretion of the Design Authority and Design Agency.

Examples can be found in DCR (document type code STP), and industry guidance can be found in IEEE Standard 1012, *IEEE Standard for Software Verification and Validation*. IEEE Standard 1012a, *IEEE Standard for Software Verification and Validation* – Supplement to 1012, may be used for additional guidance.

Refer to the SQA Documentation and Responsibility Table in Section 5.1.1 of this procedure for responsibilities. The Design Authority and Design Agency may document other applicable SQA responsibilities in the SQAP.

The Design Agency obtains the necessary input documents to generate the STP or test document. These input documents may include:

- Requirement Specification
- Requirement Traceability Matrix
- Design Document-Software
- Software test cases or test requirements.

To complete testing, modification to one or more of the documents listed above as well as the STP may be required. If so, then Design Agency shall verify the modifications are conducted in accordance with established procedures for modifying those documents.

To complete the testing, modifications to the computer program(s) being tested may be required. If the computer program(s) was baselined prior to the commencement of testing, then the Design Agency shall verify that any program modifications are conducted in accordance with established procedures and the baseline is updated.

The Design Agency shall verify that a technical review of the test procedures/plans and test results are performed.

The technical review of the test results shall verify that the test requirements have been satisfied.

The person performing the test signs the test results.

The Design Authority approves the software product for its intended use.

5.4.6 SQA Life Cycle: Installation and Acceptance Phase (Validation) [S/RID 2]

Describe how the Installation and Acceptance of the software product shall be addressed. Include in the description how the classification-dependent requirements below shall be accomplished.

Software Classification Level			SC, A			SS, B			PS, C			GS, D		
DOE O 414.1D Att 4 Sec 4	SQA ACTIVITIES	QAP 20-1	Developed	Existing	Purchased	Developed	Existing	Purchased	Developed	Existing	Purchased	Developed	Existing	Purchased
A, J	Life Cycle Phases	5.4												
H	Installation & Acceptance	5.4.6	R	R	R	R	R	R	R	G	R	G	G	G

For required ("R"), all requirements in this section shall be satisfied. If graded ("G"), consider all requirements, and document implemented requirements.

QAP 20-1 Requirements

Refer to Manual 1Q, Procedure 20-1, Section 5.4.6 for requirements.

Additional Engineering Requirements

Implementation documentation for SC/A or SS/B classification shall describe a recovery process as required if implementation fails. For other classifications apply a graded approach.

Refer to the SQA Documentation and Responsibility Table in Section 5.1.1 of this procedure for responsibilities. The Design Authority and Design Agency may document other applicable SQA responsibilities in the SQAP.

The Design Agency establishes the product baseline and turns over the software product to the Design Authority. The documentation of the acceptance of the software for operational use signifies that configuration baselines, documentation, and reviews have been completed in accordance with the SQAP.

5.4.7 SQA Life Cycle: Operations and Maintenance Phase [S/RID 2, 4]

Operation and Maintenance of the software product shall be addressed to include the description of how the classification-dependent requirements below shall be accomplished.

Software Classification Level			SC, A			SS, B			PS, C			GS, D		
DOE O 414.1D Att 4 Sec 4	SQA ACTIVITIES	QAP 20-1	Developed	Existing	Purchased	Developed	Existing	Purchased	Developed	Existing	Purchased	Developed	Existing	Purchased
A, J	Life Cycle Phases	5.4												
H, I	Operations & Maintenance	5.4.7	R	R	R	R	R	R	G	G	G	G	G	G

5.4.7 SQA Life Cycle: Operations and Maintenance Phase, [S/RID 2, 4] (cont.)

For required ("R"), all requirements in this section shall be satisfied. If graded ("G"), consider all requirements, and document implemented requirements.

QAP 20-1 Requirements

Refer to Manual 1Q, Procedure 20-1, Section 5.4.7 for requirements.

Additional Engineering Requirements

Configuration Management is defined in Section 5.5.

Changes to computer programs shall be processed through the Computer Modification Tracker (CMT) process in SmartPlant Foundation, defined in Section 5.5.

The Design Authority or Design Agency can develop the CMT, both shall review and approve.

The Design Authority shall ensure the following technical reviews are completed, based on the software change being made:

- Technical Agency reviews - the DA shall determine if any Technical Agency reviews are necessary depending on the impact of the change being made.
- Design Review – All software changes shall receive some form of design review. E7-1.58 and E7-2.60 provide guidance on the type of review required.
- Design Authority Technical Review (DATR) – A DATR is required for software changes involving software functionally classified as SC, SS, Level A or Level B or as specified in the SQAP.

The Design Authority shall ensure completion of the appropriate level of Unreviewed Safety Question (USQ) or Management of Safety Basis (MSB) review in accordance with Manual 11Q, Procedure 1.05 or 1.07, as appropriate.

Refer to the SQA Documentation and Responsibility Table in Section 5.1.1 of this procedure for responsibilities. The Design Authority and Design Agency may document other applicable SQA responsibilities in the SQAP.

5.4.8 SQA Life Cycle: Retirement Phase

During the retirement phase, the support for a software product shall be terminated and the routine use of the software prevented.

- Cyber security, risk, and safety impacts shall be verified.
- The software classification process shall be used to document the software as retired.
- A retirement plan or checklist should be developed and documented.

5.4.8 SQA Life Cycle: Retirement Phase, (cont.)

Software Classification Level			SC, A			SS, B			PS, C			GS, D		
DOE O 414.1D Att 4 Sec 4	SQA ACTIVITIES	QAP 20-1	Developed	Existing	Purchased	Developed	Existing	Purchased	Developed	Existing	Purchased	Developed	Existing	Purchased
A, J	Life Cycle Phases	5.4												
C	Retirement	5.4.8	R	R	R	R	R	R	G	G	G	G	G	G

For required ("R"), all requirements in this section shall be satisfied. If graded ("G"), consider all requirements, and document implemented requirements.

QAP 20-1 Requirements

Refer to Manual 1Q, Procedure 20-1, Section 5.4.8 for requirements.

Additional Engineering Requirements

The Design Agency terminates support and prevents routine use of the software product.

The Design Authority documents retirement of software using SWCD OSR 19-337 process.

A Retirement checklist should be developed and documented by the Design Agency and approved by the Design Authority. The details can be a section within the SQAP or a separate document referenced by the SQAP.

Refer to the SQA Documentation and Responsibility Table in Section 5.1.1 of this procedure for responsibilities. The Design Authority and Design Agency may document other applicable SQA responsibilities in the SQAP.

5.5 SQA Action: Software Configuration Control [S/RID 2, 4]

Configuration control shall be used to control, uniquely identify, describe, and document the configuration of each version or update of a computer program and its related documentation shall be described in implementing procedures. This includes configuration identification, change control, configuration status control, cyber security configuration management, and configuration management of support software.

Software Classification Level			SC, A			SS, B			PS, C			GS, D		
DOE O 414.1D Att 4 Sec 4	SQA ACTIVITIES	QAP 20-1	Developed	Existing	Purchased	Developed	Existing	Purchased	Developed	Existing	Purchased	Developed	Existing	Purchased
A, J	SQA Actions													
C	Configuration Control	5.5	R	R	R	R	R	R	R	R	R	G	G	G

For required ("R"), all requirements in this section shall be satisfied. If graded ("G"), consider all requirements, and document implemented requirements.

5.5 SQA Action: Software Configuration Control, (cont.)

QAP 20-1 Requirements

Refer to Manual 1Q, Procedure 20-1, Section 5.5 for requirements.

Additional Engineering Requirements

Industry guidance can be found IEEE Standard 828, *IEEE Standard for Software Configuration Management*.

Refer to the SQA Documentation and Responsibility Table in Section 5.1.1 of this procedure for responsibilities. The Design Authority and Design Agency may document other applicable SQA responsibilities in the SQAP.

Proposed changes to software shall be evaluated, documented, and approved or disapproved using the CMT process in SmartPlant Foundation (SPF). A graded approach for changes is implemented in SPF, based on the classification and the facility.

An engineering tool that meets all the requirements for Configuration/Version control shall be used.

5.6 SQA Action: Evaluation [S/RID 2]

This section describes the requirements for the evaluation of Existing software, or other acquired software.

Existing software is software in use at SRS that was not developed using an approved SQA program and once discovered shall be evaluated, and based on the software classification, the required SQA rigor applied to continue use of the software at SRS.

Other Acquired software is software not developed at SRS and not acquired through the site procurement process. This software shall be evaluated and placed under the SQA program.

Software Classification Level			SC, A			SS, B			PS, C			GS, D		
DOE O 414.1D Att 4 Sec 4	SQA ACTIVITIES	QAP 20-1	Developed	Existing	Purchased	Developed	Existing	Purchased	Developed	Existing	Purchased	Developed	Existing	Purchased
A, J	SQA Actions													
D	Evaluation	5.6	NA	R	G	NA	R	G	NA	R	G	NA	R	G

For required ("R"), all requirements in this section shall be satisfied. If graded ("G"), consider all requirements, and document implemented requirements. ("N/A") means not applicable.

QAP 20-1 Requirements

Refer to Manual 1Q, Procedure 20-1, Section 5.6 for requirements.

5.6 SQA Action: Evaluation, [S/RID 2] (cont.)

Additional Engineering Requirements

If the software evaluation determines that any portion of the software product shall be redeveloped or that any lifecycle activity tasks/deliverables be reconstructed or reconstituted, then those tasks/deliverables shall be identified in the SQAP in accordance with the requirements of this procedure.

Refer to the SQA Documentation and Responsibility Table in Section 5.1.1 of this procedure for responsibilities. The Design Authority and Design Agency may document other applicable SQA responsibilities in the SQAP.

The Design Agency and Design Authority shall perform and document an evaluation. This evaluation may be documented using the Software Evaluation/ Dedication Plan (SEP) or in another document such as a work request, plan, procedure, or a project level instruction, as appropriate. Examples of SEP's (previously called the Software Evaluation Plan) can be found in DCR (document type code SEP) as a starting point.

A listing shall be created of documents and software that constitute the baseline.

Place documents and source/executable code under Software Configuration Control.

5.7 SQA Action: Procurement [S/RID 2]

5.7.1 SQA Action: Procurement (Acquiring software via the Procurement Process)

Prior to procurement of Purchased Software, the classification process shall be completed to determine the level of rigor required in the procurement process for any software or equipment that contains software as a component.

Purchased software is acquired software, using the SRS procurement process and SQA process to acquire and implement the software for use at SRS.

Software Classification Level			SC, A			SS, B			PS, C			GS, D		
DOE O 414.1D Att 4 Sec 4	SQA ACTIVITIES	QAP 20-1	Developed	Existing	Purchased	Developed	Existing	Purchased	Developed	Existing	Purchased	Developed	Existing	Purchased
D	Procurement Level	5.7.1	NA	NA	1	NA	NA	2	NA	NA	3	NA	NA	3

Based on site procurement procedures, the numbers 1, 2, and 3 in the chart refer to procurement levels (see Manual 1Q, Procedure 7-2, *Control of Purchased Items and Services*, for additional information on procurement levels).

QAP 20-1 Requirements

Refer to Manual 1Q, Procedure 20-1, Section 5.7.1 for requirements.

5.7.1 SQA Action: Procurement (Acquiring software via the Procurement Process), (cont.)

Additional Engineering Requirements

Refer to the SQA Documentation and Responsibility Table in Section 5.1.1 of this procedure for responsibilities. The Design Authority and Design Agency may document other applicable SQA responsibilities in the SQAP.

Procurement level 1 and 2 for software (SC/A or SS/B) shall be from a qualified (SRS) supplier or requires Commercial Grade Dedication (CGD).

Procurement level 3 for software (PS/C or GS/D) requires a software evaluation and / or using the graded approach, a CGD process and documentation, as applicable.

5.7.2 SQA Action: Commercial Grade Dedication

NOTE

ASME NQA-1 2012 *Guidance on the Utilization of Commercial Grade Computer Programs and Software Services*, EPRI Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications (TR-106439), and DOE-EM Guidance for Commercial Grade Dedication (April 2011) can be used as guides.

Dedication methods and documentation of Purchased Software shall be prepared based on the software classification and intended use of the software.

Software Classification Level			SC, A			SS, B			PS, C			GS, D		
DOE O 414.1D Att 4 Sec 4	SQA ACTIVITIES	QAP 20-1	Developed	Existing	Purchased	Developed	Existing	Purchased	Developed	Existing	Purchased	Developed	Existing	Purchased
A, J	SQA Actions													
D	Dedication of Commercial Grade	5.7.2	NA	NA	R	NA	NA	R	NA	NA	G	NA	NA	G

Purchase options (See section 5.7.1).

For required ("R"), all requirements in this section shall be satisfied.

QAP 20-1 Requirements

See Manual 1Q, Procedure 20-1, Section 5.7.2.

5.7.2 SQA Action: Commercial Grade Dedication, (cont.)

Additional Engineering Requirements

Commercial Grade Dedication (CGD) shall be documented in a CGD Plan. See Attachment 8.2 for guidance in developing a CGD Plan. The attachment includes a description of potential Critical Characteristics for Acceptance (CCFA).

CGD is required for software classified as SC/A, SS/B..

CGD involves comparing intended function(s) vs. supplier design, verifying software meets functional requirements and Critical Characteristics, and establishing acceptance criteria.

CGD consists of two phases: Technical Evaluation and Dedication/Acceptance.

Technical Evaluation Phase

In the Technical Evaluation phase, the Safety Classification and Safety Functions shall be identified and specified in the CGD Plan.

Critical Characteristics that must be satisfied for acceptance and the methods for verifying acceptance shall also be identified in the CGD Plan.

Safety Function(s) are those functions that the software must perform to ensure safety. The Safety Function(s) are often a subset of the software functions.

Safety Functions are defined in the Documented Safety Analysis (DSA) for an existing facility or in the Preliminary Documented Safety Analysis (PDSA) for a facility under construction.

Critical Characteristics are important design and performance characteristics of a commercial grade software package that, once verified, will provide reasonable assurance that the software will perform its intended safety function.

The Critical Characteristics are in five categories: Software Identification Critical Characteristics, Host System Critical Characteristics, Interface Critical Characteristics, Software Critical Characteristics, and Vendor Critical Characteristics.

- Software Identification Critical Characteristics are important identification characteristics that uniquely identify the software being dedicated.
- Host System Critical Characteristics are the important characteristics of the host hardware and software operating environment that are required for the software.
- Interface Critical Characteristics are the important characteristics of the inputs, outputs and user interface.
- Software Critical Characteristics are the important characteristics of the software relative to performance, failure modes and functionality.
- Vendor Critical Characteristics are the important characteristics for vendor support, vendor qualifications and vendor quality assurance program.

5.7.2 SQA Action: Commercial Grade Dedication, (cont.)

Technical Evaluation Phase, (cont.)

Software Classification and Requirements for the Software shall be determined, documented, and approved before procurement.

Like-for-Like Replacement for software is a reinstallation of the same exact software from the same distribution media onto a system with the same exact operating system with the same configuration and patches.

Equivalent Replacement for software is when there are no changes in design, implementation, or function that could prevent the replacement software from being interchangeable under the design condition of the original software and performing its required safety function.

Refer to the SQA Documentation and Responsibility Table in Section 5.1.1 of this procedure for responsibilities. The Design Authority and Design Agency may document other applicable SQA responsibilities in the SQAP.

- A Commercial Grade Dedication Plan shall be developed by the Design Agency and Design Authority.
- The Design Agency and Design Authority shall perform the Technical Evaluation.
- The Design Agency shall generate the Requirements Traceability Matrix (RTM) which will identify many of the Critical Characteristics in the Host System, Interface, and Software categories.
- The Design Agency and Design Authority shall perform and document the CGD process.

Dedication/Acceptance Phase

For acquisition of Commercial Grade Software, determine acceptance methods based on acceptance criteria, available supplier information, quality history, and degree of standardization.

Four methods have been identified that shall be used to verify that the Critical Characteristics have been met and the Software meets CDG requirements.

More than one of these methods should be used as specified in the CGD Plan to verify the Acceptance Criteria of each CC.

For Software CGD, Method 1 is always used unless the site Chief Engineer approves an exception.

5.7.2 SQA Action: Commercial Grade Dedication, (cont.)

Method 1 - Special Tests, Inspections, or Analyses

Special Tests, Inspections, or Analyses are special test, inspection or analyses conducted either individually or in combination upon or after receipt of the software to verify conformance with the acceptance criteria.

Method 1 may be potentially used alone for the following:

- When Critical Characteristics are able to be verified with tests/inspections
- When data to verify Critical Characteristics is available in existing documents such as specifications, drawings, software life cycle documents, instruction manuals, and catalogs
- When the software does not include functionality beyond the safety functions
- When post-installation tests can be conducted (Testing the software in the SRS environment).

Other Methods should be considered and used with Method 1 to complete the CGD process.

Method 2: Commercial Grade Survey

A Commercial Grade Survey is a survey of a supplier to dedicate software based on approval of a suppliers' implementing process and commercial controls as related to the Critical Characteristics when ASME NQA-1 is not invoked in the purchase order

The survey of the supplier shall be performed and deemed acceptable prior to issuing the purchase order for the software.

A survey of a supplier may be appropriate:

- When the supplier/manufacturer has implemented appropriate, documented commercial controls over the Critical Characteristics (as verified by the commercial grade survey)
- When multiple software items are being procured from the same supplier
- When Critical Characteristics are not easily verified after receipt.

Method 3 - Source Verification

Source verification is a method of acceptance conducted at the supplier's facility or other applicable location to verify conformance with the identified Critical Characteristics and acceptance criteria during the development process.

The scope of the source verifications shall include activities such as witnessing the development of the software, performance tests, or final inspections, as applicable. It shall also include verification of the supplier's design, as applicable to the identified Critical Characteristics.

5.7.2 SQA Action: Commercial Grade Dedication, (cont.)

Method 3 - Source Verification, (cont.)

Source verification shall be performed in accordance with a checklist or plan with the documented evidence of the source verification furnished to the dedicating entity for approval and shall include or address the following:

- Identification of the software included within the scope of the source verification
- Identification of the Critical Characteristics, including acceptance criteria being controlled by the supplier
- Verification that the supplier's processes and controls are effectively implemented for the identified Critical Characteristics
- Identification of the activities witnessed during the source verification and the results obtained
- Documentation of the adequacy of the supplier's processes and controls associated with the Critical Characteristics and acceptance.

When using source verification, Critical Characteristics are verified by witnessing the quality activities of the supplier specific to the software being dedicated before the software is released for shipment

Source verification may be appropriate:

- When in-process verification of one or more Critical Characteristics is needed
- When non-conformances have been detected during prior receipt inspections
- When problems/deficiencies exist with the supplier's quality assurance program/procedures
- Buyer schedule demands
- Software development requires a significant amount of time
- Software being procured is the first of its kind being developed.

Method 4 - Acceptable Supplier Item or Service Performance Record

Acceptable Supplier Item or Service Performance Record is a method of acceptance that is based upon the documented, demonstrated past performance of supplied software over a period of time for similar software products.

Before using Method 4 as a means to justify that quality can be assured using the CGD process, the dedicating entity needs to understand that this method is considered to be very difficult to implement as a stand-alone method of acceptance. For software, CGD method 4:

- Shall not rely on a single source of information
- Shall not be used as the sole method of acceptance.

Method 4 shall not be used unless it is in conjunction with Methods 1, 2, and/or 3.

5.7.2 SQA Action: Commercial Grade Dedication, (cont.)

Method 4 - Acceptable Supplier Item or Service Performance Record, (cont.)

Method 4 is a means to assist in accepting software since it relies on documented historical performance and may not require costly and time-consuming inspection and auditing activities.

Use of Method 4 allows the purchaser to accept software based upon a confidence in the supplied software achieved through proven performance of similar software.

Method 4 requires documented historical performance:

- Cannot be used if the only history available is with the purchaser
- Should only be used when a large dataset of successful historical performance for the software is available
- When Critical Characteristics are not easily verified after receipt
- Verify historical performance data that used Methods 1, 2, or 3 for similar software
- Verify that the performance data used is directly applicable to the verification of Critical Characteristics specific to the intended application
- Verify performance record is from similar condition of service, environmental condition, failure mode, maintenance program, testing, or other conditions equivalent to the intended application of the software
- In the application of this method proper care should be exercised to verify that the performance data used is directly applicable to the verification of Critical Characteristics specific to the intended application
- Monitored performance of the software installed and operated in a similar environment as the intended facility.

Third-Party Evaluation:

- Industry Wide Performance - Shall be specific and applicable to the software being accepted
- Commercial Program Audits/Surveys Conducted by Industry Groups
- Industry product test and Industry databases (INPO, EPRI, Aerospace, Military etc.)
- Utilization of National Codes and Standards.

5.8 SQA Action: Problem Reporting and Corrective Action

Conditions adverse to quality shall be identified promptly and corrected as soon as practicable.

Software Classification Level			SC, A			SS, B			PS, C			GS, D		
DOE O 414.1D Att 4 Sec 4	SQA ACTIVITIES	QAP 20-1	Developed	Existing	Purchased	Developed	Existing	Purchased	Developed	Existing	Purchased	Developed	Existing	Purchased
A, J	SQA Actions													
I	Problem Reporting & Corrective Action	5.8	R	R	R	R	R	R	G	G	G	G	G	G

For required ("R"), all requirements in this section shall be satisfied. If graded ("G"), consider all requirements, and document implemented requirements.

QAP 20-1 Requirements

Refer to Manual 1Q, Procedure 20-1, Section 5.8 for requirements.

Additional Engineering Requirements

For existing and developed software, define methods for reporting operational software problems and programmatic deficiencies, and taking appropriate corrective action.

For purchased software, identify requirements for Supplier's reporting of software problems to the Purchaser and the Purchaser's reporting of software problems to the Supplier.

For freely acquired software, define methods for receiving reports of operational software problems and programmatic deficiencies, and define methods for taking appropriate corrective action.

Refer to the SQA Documentation and Responsibility Table in Section 5.1.1 of this procedure for responsibilities. The Design Authority and Design Agency may document other applicable SQA responsibilities in the SQAP.

5.9 SQA Action: Software Security Controls / Cyber Security Control

Requirements of Manual 10Q, *Cyber Security Manual*, and Manual 7Q, *Security Manual*, are applied as required.

The cyber security mitigation strategies shall be implemented to permit authorized and to prevent unauthorized access to the system.

Software Classification Level			SC, A			SS, B			PS, C			GS, D		
DOE O 414.1D Att 4 Sec 4	SQA ACTIVITIES	QAP 20-1	Developed	Existing	Purchased	Developed	Existing	Purchased	Developed	Existing	Purchased	Developed	Existing	Purchased
A, J	**SQA Actions**													
B, G	Cyber Security Controls	5.9	CS	CS	CS	CS	CS	CS	CS	CS	CS	CS	CS	CS

("CS") means cyber security requirements.

QAP 20-1 Requirements

Refer to Manual 1Q, Procedure 20-1, Section 5.9 for requirements.

Additional Engineering Requirements

The methods to be used to permit authorized and prevent unauthorized access to the system shall be documented in the SQA documentation and / or in the related cyber security documentation.

The Design Agency shall verify that access controls comply with applicable site automated data processing system security requirements specified in Manual 10Q unless otherwise documented and justified in the SQAP or other cyber security related documentation.

Newly developed or acquired software shall be incorporated into a Certification and Accreditation (C&A) Project or Accreditation Boundary and evaluated against security requirements for the identification of risks and development of associated mitigations.

The Design Agency shall verify the Accreditation Boundary (AB) requirements and implement as required.

Refer to the SQA Documentation and Responsibility Table in Section 5.1.1 of this procedure for responsibilities. The Design Authority and Design Agency may document other applicable SQA responsibilities in the SQAP.

5.10 SQA Action: Safety Software Inventory List (SSIL)

As part of the SWCD software classification process, the Design Authority determines if the software is safety software that should be included on the SSIL.

The Site Quality Assurance Manager is responsible for maintaining the SSIL (per Manual 1Q, Procedure 20-1). The SWCD application provides the majority of the SSIL with additional SSIL items not in the SWCD on the QA webpage.

Software Classification Level			SC, A			SS, B			PS, C			GS, D		
DOE O 414.1D Att 4 Sec 4	SQA ACTIVITIES	QAP 20-1	Developed	Existing	Purchased	Developed	Existing	Purchased	Developed	Existing	Purchased	Developed	Existing	Purchased
A, J	Safety Software Inventory List (SSIL)	5.10	ALL SOFTWARE THAT MEETS ONE OF THE THREE SSIL DEFINITIONS WILL BE MAINTAINED BY QA											

QAP 20-1 Requirements

Refer to Manual 1Q, Procedure 20-1, Section 5.2 Items 8 & 9, and Section 5.10 for requirements.

Additional Engineering Requirements

The Design Agency can recommend the SSIL determination and then verifies documentation is complete. The safety software determination is based on the requirements identified in DOE Order 414.1C/414.1D, Manual 1Q, Procedure 20-1, and the Quality Assurance Management Plan (QAMP).

Refer to the SQA Documentation and Responsibility Table in section 5.1.1 of this procedure for responsibilities. The Design Authority and Design Agency may document other applicable SQA responsibilities in the SQAP.

5.11 SQA Action: Data Management [S/RID 2]

Manual 1Q, Procedure 20-1 does not directly address the issue of Data Management Plans (DMP). A DMP template is in SRNS-IM-2011-00048, *Software Quality Assurance (SQA) Documentation Template Examples*.

Additional Engineering Requirements

The Design Authority or Data Owner may request a Data Management Plan for any data that is created, managed, or used by any classification of software.

The SQAP or DMP shall clarify the roles and responsibilities. The "or" in the statements below shall be assigned to the Design Authority or Design Agency in the SQAP or DMP, so responsibility is clarified.

The Design Authority or Design Agency evaluates the availability, quality and accuracy of the data created and modified within respective business processes and determines the level of data management required.

The Design Authority or Design Agency determines the need for and, if needed, obtains an Authorized Derivative Classifier/Reviewing Official (ADC/RO) review.

The Design Authority or Design Agency reviews and approves requests submitted by data users.

The Design Agency verifies data security requirements are documented to satisfy the requirements.

Changes are processed via SPF [CMT/Data Modification Tracker (DMT)], or comparable change control method, to manage changes to data, including detection of data errors, data change requests, or new data requirements.

6.0 REFERENCES

NOTE

IHS is a service available through the site engineering webpage to obtain access to industry standards and guides such as ASME NQA-1, and IEEE.

1B, *Management Requirements and Procedures*

1B, 3.31, *Records Management*

1Q, *Quality Assurance*

1Q, 20-1 Software Quality Assurance

7Q, *Security Manual*

6.0 REFERENCES, (cont.)

10Q, *Cyber Security Manual*

ASME NQA-1 2012 *Guidance on the Utilization of Commercial Grade Computer Programs and Software Services* (Draft)

DOE EM Guidance for Commercial Grade Dedication, April 2011

E7, *Conduct of Engineering*

E7, 1.20, *Engineering Document Numbering System*

E7, 2.05, *Modification Traveler*

E7, 2.25, *Functional Classifications*

E7, 2.60, *Technical Reviews*

E7, 3.46, *Replacement Item Evaluation / Commercial Grade Dedication*

E11, *Project Management*

Institute of Electrical and Electronics Engineers (IEEE) Standard 730, *IEEE Standard for Software Quality Assurance Plans*,

IEEE Standard 730.1, *IEEE Guide for Software Quality Assurance Planning*.

IEEE Standard 828, *IEEE Standard for Software Configuration Management*.

IEEE Standard 830, *IEEE Recommended Practice for Software Requirements Specifications*

IEEE Standard 1012, *IEEE Standard for Software Verification and Validation*

IEEE Standard 1012a, *IEEE Standard for Software Verification and Validation*

IEEE Standard 1016, *IEEE Recommended Practice for Software Design Descriptions*

IEEE Standard 1016.1, *IEEE Guide to Software Design Descriptions.*

IEEE Standard 1058, IEEE *Software Project Management Plans*

IEEE Standard 1233, IEEE *Guide for Developing System Requirements*

[S/RID 1], (Standards/Requirements Identification Documents) DOEO414.1D, *Quality Assurance*

[S/RID 2], DOE/RW-0333PR20, *Quality Assurance Requirements and Description*

[S/RID 3], DOE/NNSA QC-1, Rev. 10, *DOE/NNSA QC-1 Weapon Quality Policy QC-1*

[S/RID 4], DOEO420.1B, *Facility Safety*

6.0 REFERENCES, (cont.)

SRNS IM-2011-00003, *Commercial Grade Dedication Guidance Manual*

SRNS IM-2011-00048, *Software Quality Assurance (SQA) Documentation Template Examples*

TR-106439, *EPRI Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications*

7.0 RECORDS

Any records generated as a result of performing this procedure shall be maintained in accordance with Manual E7, Procedure 1.20, *Engineering Document Numbering System*, and Manual 1B, Procedure 3.31, *Records Management*.

8.0 ATTACHMENTS

Attachment 8.1 DOE Order 414.1C/414.1D SSQA Work Activities

Attachment 8.2 Commercial Grade Dedication Plan for Software

ATTACHMENT 8.1
DOE Order 414.1C/414.1D SSQA Work Activities
Page 1 of 1

Using the consensus standard selected (ASME NQA-1) and the grading levels established and approved (in QAMP), select and implement applicable SSQA work activities from the list below.

Activity	Description
A	Software project management and quality planning
B	Software risk management
C	Software configuration management
D	Procurement and supplier management
E	Software requirements identification and management
F	Software design and implementation
G	Software safety analysis and safety design methods
H	Software verification and validation
I	Problem reporting and corrective action
J	Training of personnel in the design, development, use and evaluation of safety software

ATTACHMENT 8.2
Commercial Grade Dedication Plan for Software
Page 1 of 27

TECHNICAL EVALUATION / APPROVAL

"Section 1 and the Technical Evaluation portion of Section 2 was properly performed and established the basis for acceptance."

Design Authority_____ QA(if required)_____
Printed Name Printed Name

Date _____ Date _____

Signature_____ Signature_____

Design Agency_____ IR(if required)_____
Printed Name Printed Name

Date_____ Date _____

Signature_____ Signature_____

DEDICATION AND ACCEPTANCE APPROVAL

"For each identified Critical Characteristic in Section 2, the Acceptance portion has been completed. Therefore, the software is considered dedicated."

Design Authority_____ QA(if required)_____
Printed Name Printed Name

Date _____ Date _____

Signature_____ Signature_____

Design Agency_____ IR(if required)_____
Printed Name Printed Name

Date_____ Date _____

Signature_____ Signature_____

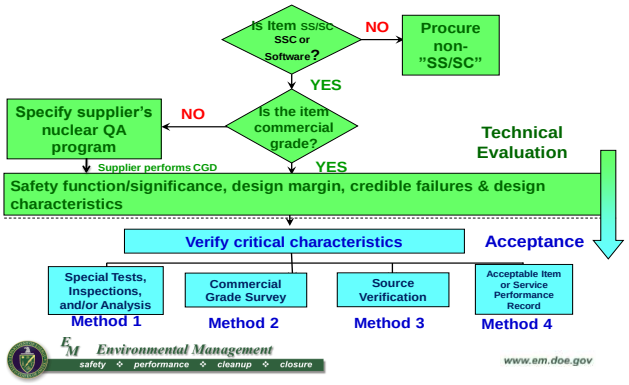
ATTACHMENT 8.2
Commercial Grade Dedication Plan for Software
Page 2 of 27

COMMERCIAL GRADE DEDICATION OVERVIEW

A commercial grade dedication plan is established to document the technical evaluation, including the identification of the critical characteristics for acceptance, and the methods for acceptance. This plan was developed to comply with requirements of ASME NQA-1a-2009, Part II, Subpart 2.14 for software. A separate CGD may be required for other components of the safety system.

Software CGD follows a two-phase approach. In the Technical Evaluation phase, the software is classified, safety functions are specified and the need for CGD is determined. This is performed by completing Section 1 of this document. Technical Evaluation also completes the Technical Evaluation portions of Section 2. This includes specifying all of the Critical Characteristics for Acceptance (CCFA), their Acceptance Criteria and the Method of Verification that is to be used for acceptance. The Design Authority, Design Agency, QA and IR (if required) approve the Technical Evaluation by signing and dating the cover page.

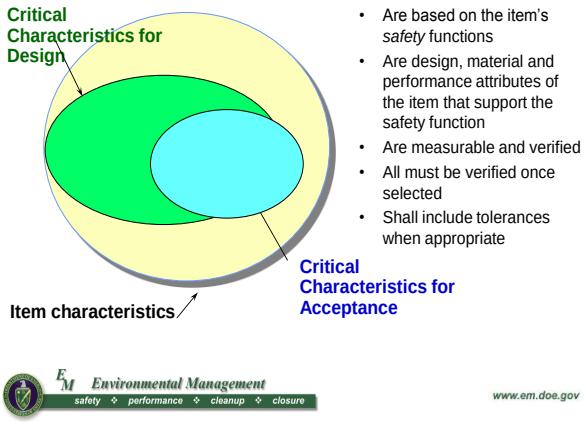
Overview of the Generic CGD Process



During the Acceptance phase, the specified methods of verification are used to ensure that all of the CCFAs meet their Acceptance Criteria. Acceptance is documented in Section 2 by specifying the individual who performed the verification and when the verification was performed. The Design Authority, Design Agency, QA and IR (if required) approve the Acceptance by signing and dating the cover page.

Commercial Grade software can have numerous characteristics that are related to composition, identification, or performance and may or may not impact its safety function. The Critical Characteristics for Design (CCFD) are those design characteristics that are important to the performance of the software that allows it to perform its safety function. However, it is not normally prudent or fiscally sound to verify all item characteristics and/or CCFD to provide reasonable assurance that the software will perform its intended safety function. Critical Characteristics for Acceptance (CCFA) are identifiable and measurable attributes of an item or service that, when verified, will provide reasonable assurance that the item/service received is the item specified. Reasonable assurance is considered to have been provided when, in the opinion of the responsible engineer, a sufficient number of CCFD and item characteristics have been verified and documented as CCFA to cause one to believe that the item will be capable of performing its safety function.

Critical Characteristics for Acceptance



- Are based on the item's *safety* functions
- Are design, material and performance attributes of the item that support the safety function
- Are measurable and verified
- All must be verified once selected
- Shall include tolerances when appropriate

ATTACHMENT 8.2
Commercial Grade Dedication Plan for Software
Page 3 of 27

1. TECHNICAL EVALUATION

The technical evaluation shall be performed by engineering and used to identify and document the safety function of each item/service based on review of the approved safety analysis and supporting data. The complete Technical Evaluation is based on the information in the following subsections. Dedication requirements shall be included in applicable procurement and technical documents as necessary to support the dedication.

1.1. Commercial Grade Information

Supplier Identification:

Includes description, supplier name and unique identifier, if applicable.

Software Description:

Includes an end use text description of the software including the design functions for the selected application.

1.2. Safety Function

Safety Functions – Specify the safety function(s) performed by the software in support of the overall safety function as described in the Documented Safety Analysis (DSA) for an existing facility or in the Preliminary Documented Safety Analysis (PDSA) for a facility under construction. The function(s) is/are often a subset of the software function. If there is any question as to the safety function, the question should be raised to the responsible engineer to ensure the proper determination of safety function.

1. Primary Safety Function:

2. Secondary Safety Function (If any):

Effect on Assembly/System Safety Function (e.g. embedded controller):

ATTACHMENT 8.2
Commercial Grade Dedication Plan for Software
Page 4 of 27

1.3. Safety Function References

Specify the references used to identify the safety function(s) as part of the Technical Evaluation. Additional objective evidence can be attached to this CGD Plan.

Document Type	**Document Number**
Documented Safety Analysis (PDSA/DSA):	
OSR 19-337 SWCD Document:	
Software Quality Assurance Plan:	
Requirements Documentation:	
Other Documentation:	
Applicable Drawings:	

1.4. Safety Classification

Complete software classification to determine whether CGD is required for the software.

1. Is this software classified as SC/A Safety Class? [ ] Yes [ ] No

2. Is this software classified as SS/B Safety Significant? [ ] Yes [ ] No

If the answer is ”Yes” to either question, CGD is required. Continue with developing the plan. If all answers are “No”, CGD is not required.

1.5. Commercial Grade Item Determination

Was the software created by an SRNS Qualified Supplier?

[ ] Yes (The item does not need CGD) [ ] No (Continue to Section 1.6)

1.6. Like-for-like Replacement Item

Part II, Subpart 2.14, paragraph 402 states that for a software product to be like-for-like, the following condition must be satisfied:
Is this a reinstallation of the same exact software from the same distribution media onto a system with the same exact operating system with the same configuration and patches?

[ ] Yes (New CGD is not required) [ ] No (Proceed to Section 1.7)

ATTACHMENT 8.2
Commercial Grade Dedication Plan for Software
Page 5 of 27

1.7. Equivalent Replacement Item

Are there changes in design, implementation, or function that could prevent the replacement software from being interchangeable under the design condition of the original software and performing its required safety function? (ASME NQA-1a-2009, Part II, Subpart 2.14, Section 403) (e.g., major software update, platform change, change in vendor)

[ ] Yes [ ] No

If “Yes”, then the replacement software is not equivalent. The software must be rejected under the existing CGD Plan or processed as a design change.

If “No”, then the replacement software may be equivalent. Selection and verification of the identified critical characteristics by an appropriate dedication method(s) is required in accordance with the existing CGD Plan.

ATTACHMENT 8.2
Commercial Grade Dedication Plan for Software
Page 6 of 27

2.0 IDENTIFY AND VERIFY THE CRITICAL CHARACTERISTICS FOR ACCEPTANCE

Based on the Technical Evaluation, number and identify the Critical Characteristics for Acceptance (CCFA) that are required for Acceptance. Specify the Acceptance Criteria and the number of the appropriate Method of Verification that is to be used. Section 3 describes the four Methods of Verification. Section 4 contains some example Critical Characteristics.

During Acceptance, the individual who performed the verification shall sign and date each CCFA they verified.

The Critical Characteristics for Acceptance, Acceptance Criteria and Method of Verification may be specified in this document or in the Requirements Traceability Matrix document. If the RTM is used, it must be referenced or attached to the CGD Plan and contain that same information as shown in the table below.

The following sub-sections specify categories that should be considered for software CGD. Example CCs for each of these categories is provided in Section 4. Not all CCs examples are required for all software CGD Plans.

Reasonable assurance is considered to have been provided when, in the opinion of the responsible engineer, a sufficient number of CCFD and item characteristics have been verified and documented as CCFA to cause one to believe that the item will be capable of performing its safety function.

2.1. Software Identification Critical Characteristics

Verify through inspection that the identifying critical characteristics are the same as listed on the procurement document. Other identifying characteristics may be used.

Technical Evaluation					***Acceptance***	
#	***CCFA***	***Description***	***Acceptance Criteria***	***Method of Verification***	***Verified by***	***Date***
1	Software Name		Software Name	1		
2	Software Version Identifier		Software Version Identifier	1		
3	Receipt Media		Receipt Media	1		

ATTACHMENT 8.2
Commercial Grade Dedication Plan for Software
Page 7 of 27

2.2. Host System Critical Characteristics

The specific host system characteristics may be CCFAs if they are required to properly execute the software.

2.2.1. Host Computer Hardware

The following CCs define the requirements for the host computer hardware that the software will be install on:

Technical Evaluation					*Acceptance*	
#	*CCFA*	*Description*	*Acceptance Criteria*	*Method of Verification*	*Verified by*	*Date*

2.2.2. Operating System and Configuration

The following CCs define the requirements for the host computer operating system and system configuration:

Technical Evaluation					*Acceptance*	
#	*CCFA*	*Description*	*Acceptance Criteria*	*Method of Verification*	*Verified by*	*Date*

2.2.3. Recovery (Portability)

The following CCs define the recovery requirements in the event of a system failure:

Technical Evaluation					*Acceptance*	
#	*CCFA*	*Description*	*Acceptance Criteria*	*Method of Verification*	*Verified by*	*Date*

2.3. Interface Critical Characteristics

The following CCs define the interface requirements of the software:

Technical Evaluation					*Acceptance*	
#	*CCFA*	*Description*	*Acceptance Criteria*	*Method of Verification*	*Verified by*	*Date*

ATTACHMENT 8.2
Commercial Grade Dedication Plan for Software
Page 8 of 27

2.4 Software Critical Characteristics

CCFAs that pertain to the software's functionality may include its performance, its "must-not-do" functions, its expected failure modes and specific functional characteristics.

2.4.1 Performance

The engineer shall, as part of the Technical Evaluation, determine if there are specific performance expectations that must be met by the software to perform the safety function.

Performance characteristics can also include characteristics related to failure management and "must-not-do" functions.

Technical Evaluation					*Acceptance*	
#	*CCFA*	*Description*	*Acceptance Criteria*	*Method of Verification*	*Verified by*	*Date*

Performance Requirements – Determine if there are specific performance expectations that must be met by the software to implement its safety function effectively. This can include throughput, sample rate, response-time, or any real-time requirement.

Technical Evaluation					*Acceptance*	
#	*CCFA*	*Description*	*Acceptance Criteria*	*Method of Verification*	*Verified by*	*Date*

2.4.2. Failure Modes

Failure analysis provides information that assists in evaluating and verifying critical characteristics. It is important to understand the failure modes of the commercial device and their impact on the system failure modes. Failure analysis supports CGD as well as design. Consideration of potential failure modes and mechanisms helps to identify critical characteristics.

Technical Evaluation					*Acceptance*	
#	*CCFA*	*Description*	*Acceptance Criteria*	*Method of Verification*	*Verified by*	*Date*

2.4.3. Functionality Critical Characteristics

The following CCs define the functionality of the software:

Technical Evaluation					*Acceptance*	
#	*CCFA*	*Description*	*Acceptance Criteria*	*Method of Verification*	*Verified by*	*Date*

ATTACHMENT 8.2
Commercial Grade Dedication Plan for Software
Page 9 of 27

2.5. Vendor Critical Characteristics

This section contains CCFAs that pertain to the vendor of the software.

2.5.1. Service Conditions

The following CCs relate to the Vendor's ability to provide support of the software being dedicated:

Technical Evaluation					*Acceptance*	
#	*CCFA*	*Description*	*Acceptance Criteria*	*Method of Verification*	*Verified by*	*Date*

2.5.2. Qualifications

The following CCs define the qualification of the vendor's staff and organization:

Technical Evaluation					*Acceptance*	
#	*CCFA*	*Description*	*Acceptance Criteria*	*Method of Verification*	*Verified by*	*Date*

2.5.3. Operating History

The following CCs define the required operating history of the vendor:

Technical Evaluation					*Acceptance*	
#	*CCFA*	*Description*	*Acceptance Criteria*	*Method of Verification*	*Verified by*	*Date*

ATTACHMENT 8.2
Commercial Grade Dedication Plan for Software
Page 10 of 27

2.6. Dependability / Built-in-Quality / SQA Program

This is the category in which dedication of software differs from that of other types of items. Dependability addresses attributes that typically cannot be verified through inspection and testing alone and are generally affected by the process used to produce the item. The following is Attachment 8.2 of QAP 20-1 and shows the graded approach, based on classification for each of the SQA Activities, including Purchased software which requires CGD.

Software Classification Level			SC, A			SS, B			PS, C			GS, D		
DOE O 414.1D Att 4 Sec 4	SQA ACTIVITIES	QAP 20-1	Developed	Existing	Purchased	Developed	Existing	Purchased	Developed	Existing	Purchased	Developed	Existing	Purchased
A, J	Software Classification	5.2	R	R	R	R	R	R	R	R	R	R	R	R
A, J	SQA Procedures/Plans	5.3	R	R	R	R	R	R	R	R	R	R	R	R
A, J	**Life Cycle Phases**	5.4												
E	Requirements	5.4.2	R	R	R	R	R	R	R	G	G	G	G	G
F, G	Design	5.4.3	R	G	G	R	G	G	G	G	G	G	G	G
F	Implementation	5.4.4	R	G	G	R	G	G	G	G	G	G	G	G
H	Testing	5.4.5	R	G	R	R	G	R	G	G	G	G	G	G
H	Installation & Acceptance	5.4.6	R	R	R	R	R	R	R	G	R	G	G	G
H, I	Operations & Maintenance	5.4.7	R	R	R	R	R	R	G	G	G	G	G	G
C	Retirement	5.4.8	R	R	R	R	R	R	G	G	G	G	G	G
A, J	**SQA Actions**	5.5-5.10												
C	Configuration Control	5.5	R	R	R	R	R	R	R	R	R	G	G	G
D	Evaluation	5.6	NA	R	G	NA	R	G	NA	R	G	NA	R	G
D	Procurement Level	5.7.1	NA	NA	1	NA	NA	2	NA	NA	3	NA	NA	3
D	Dedication of Commercial Grade	5.7.2	NA	NA	R	NA	NA	R	NA	NA	G	NA	NA	G
I	Problem Reporting & Corrective Action	5.8	R	R	R	R	R	R	G	G	G	G	G	G
B, G	Risk and Safety Analysis	5.x	R	R	R	R	R	R	G	G	G	G	G	G
B, G	Cyber Security Controls	5.x	CS	CS	CS	CS	CS	CS	CS	CS	CS	CS	CS	CS
A, J	Safety Software Inventory List (SSIL)	5.2 5.10	ALL SOFTWARE THAT MEETS ONE OF THE THREE SSIL DEFINITIONS WILL BE MAINTAINED BY QA											

Definitions:

R	*= Requirement (Shall) must be met and defined in the SQAP.*
G	= A graded approach is used. Consider all requirements, document implemented requirements and justify exceptions.
CS	= Cyber Security requirements per 10Q and 7Q must be met
NA	= Not Applicable

For software-based systems, high quality is best achieved by: building it in, following a systematic life cycle approach from requirements through implementation, with verification and validation steps, and appropriate documentation for each phase of the life cycle.

- SQA Program
- Requirements Traceability
- Design
- Design for Reliability
- Independent Review

ATTACHMENT 8.2
Commercial Grade Dedication Plan for Software
Page 11 of 27

- Implementation.
- Testing
- Configuration Control
- Instruction Manual
- Maintenance
- Retirement.

Technical Evaluation					***Acceptance***	
#	***CCFA***	***Description***	***Acceptance Criteria***	***Method of Verification***	***Verified by***	***Date***

ATTACHMENT 8.2
Commercial Grade Dedication Plan for Software
Page 12 of 27

3. CGD METHOD FOR VERIFICATION/ ACCEPTANCE

Dedication Method – Provides the basis for the selection of one or more of the four available methods to verify the Critical Characteristics for Acceptance (CCFA). One or more of the four following methods shall be used to determine acceptance of the software for its intended use. Method 1 is required for software CGD. Methods 2, 3, and 4 may be used in addition to Method 1 to verify the CCFAs.

METHOD 1- SPECIAL TESTING AND/OR INSPECTION

Special Tests, Inspections, or Analyses are special test, inspection or analyses conducted either individually or in combination upon or after receipt of the software to verify conformance with the acceptance criteria.

For each Critical Characteristics that specified Method 1 and required a Special Test, describe the test in detail, the expected result and the actual results.

For each Critical Characteristics that specified Method 1 and required an Inspection, describe the inspection in detail and the actual results.

For each Critical Characteristics that specified Method 1 and required an Analysis, describe the analysis in detail, the expected result and the actual results.

METHOD 2 – COMMERCIAL GRADE SURVEY OF SUPPLIER

A Commercial Grade Survey is a survey of a supplier to dedicate software based on approval of a suppliers' implementing process and commercial controls as related to the Critical Characteristics when ASME NQA-1 is not invoked in the purchase order.

For each Critical Characteristics that specified Method 2, describe the Commercial Grade Survey in detail including the program elements to be evaluated that support the procurement. This should include referencing the supplier's implementing procedures. List the expected results and the actual results.

METHOD 3 – SUPPLIER SOURCE VERIFICATION

Source verification is a method of acceptance conducted at the supplier's facility or other applicable location to verify conformance with the identified Critical Characteristics and acceptance criteria during the development process.

For each Critical Characteristics that specified Method 3, describe the Supplier Source Verification activities in detail. These should be documented in the procurement specification as witness/hold points. List the expected results and the actual results.

METHOD 4 – SUPPLIER PERFORMANCE/HISTORY

Acceptable Supplier Item or Service Performance Record is a method of acceptance that is based upon the documented, demonstrated past performance of supplied software over a period of time for similar software products.

For each Critical Characteristics that specified Method 4, describe the Supplier Performance Record in detail and list all the referenced material that was used to develop a performance history used to determine acceptability.

NOTE: Supplier performance/history shall not be used as the only method of acceptance for software CGD.

ATTACHMENT 8.2
Commercial Grade Dedication Plan for Software
Page 13 of 27

4.0. EXAMPLE CRITICAL CHARACTERISTICS FOR ACCEPTANCE

This section presents various CC that could be used to specify the CCFAs. Not all CCs apply to all software. It is expected that there are CCs that are not listed.
Each of the sub-sections corresponds to the same sub-section in Section 2.
The Methods of Verification specified within these examples are recommendations. Depending on the particular software and CCFA, one of the other four methods of verification may be applicable.

4.1. Software Identification Critical Characteristics

Technical Evaluation				
#	***CCFAs***	***Description***	***Acceptance Criteria***	***Method of Verification***
1	Software Name	Name of software given by the supplier.	Software name	1
2	Software Version Identifier	Software version identifier, including version, build, release date and revision/patches, as available.	Software version	1
3	Receipt Media	The physical object received from the supplier that contains the software.	Software media	1

ATTACHMENT 8.2
Commercial Grade Dedication Plan for Software
Page 14 of 27

4.2. Host System Critical Characteristics

4.2.1. Host Computer Hardware

Technical Evaluation				
#	***CCFAs***	***Description***	***Acceptance Criteria***	***Method of Verification***
4	Computer Model	Description of particular computer name and model if required.	Model number	1
5	Processor type and performance	Description of processor type (e.g. x86, ARM, Xeon) if required	Type or model number	1
6	Memory capacity	Amount of memory that the computer must contain in order to run the software	Size (e.g. 4 GB)	1, 2
7	Disk capacity	Amount of disk space that is needed to install and execute the software	Size (e.g. 100 GB)	1, 2
8	I/O requirements	Detailed specification for each input and output of the system that is required to use the software	Input/output requirements (e.g. dual HD monitors, graphics card, 3 16-bit 1M Sample/second ADC's)	1
9	Ruggedness	Ability to withstand harsh environmental conditions (temperature, dust, humidity, shock, vibration, etc.)	Temperature ranges Dust conditions Humidity range Vibration conditions	1, 3

4.2.2. Operating System and Configuration

Technical Evaluation				
#	***CCFAs***	***Description***	***Acceptance Criteria***	***Method of Verification***
10	Host computer operating system identifier	Required operating system and patches/ service packs.	Manufacturer name Model number (e.g. Windows 7 SP2)	1
11	Host computer operating environment	Additional packages required to enable the software to execute.	Additional software package identifiers (e.g. Java 2.0 or greater, Matlab 7.14, LabVIEW 2012)	1

4.2.3. Recovery (Portability)

Technical Evaluation				
#	***CCFAs***	***Description***	***Acceptance Criteria***	***Method of Verification***
12	Environmental Compatibility: Recovery	If required to meet the safety function(s), the measure of the effort/time required to migrate the software to an equivalent hardware platform, component or environment.	Measure of effort or time (e.g. 30 seconds, 5 minutes, 12 hours)	1

ATTACHMENT 8.2
Commercial Grade Dedication Plan for Software
Page 15 of 27

4.3. Interface Critical Characteristics

Technical Evaluation				
#	***CCFAs***	***Description***	***Acceptance Criteria***	***Method of Verification***
13	Interfaces: Critical input parameters and valid ranges	The set of input parameters and the valid range of their valid values	Input parameters with valid ranges	1, 3, 4
14	Interfaces: Critical outputs	The characteristics of the critical output parameters. For example, design and analysis software might include file formats, whereas embedded systems/controllers might include signal specification, signal strength, signal type.	Output parameters	1, 3, 4
15	Accuracy/ Precision/ Tolerance Outputs	For accuracy: the degree in which there is a close correlation with the expected or desired outcome. (e.g., +/- 1% compared to specified reference) For precision: the degree of repeatability or degree of measure. (e.g. 32-bit IEEE floating point) For tolerance: the allowable error in measurement.	Accuracy/ precision/ tolerance of outputs	1, 3, 4
16	Interfaces: User Interface Compatibility	The software user interface design that provides consistency, including the use of symbols, notations, terminology, conventions, and layout. (e.g. control system interface GUI)	Description of the type of user interface and required conventions	1

ATTACHMENT 8.2
Commercial Grade Dedication Plan for Software
Page 16 of 27

4.4. Software Critical Characteristics

4.4.1. Performance

Technical Evaluation				
#	*CCFAs*	*Description*	*Acceptance Criteria*	*Method of Verification*
17	Response Time	Specify Response time for each critical action. Response time is the time in which it takes the software to execute a specific action.	Response time	1
18	Throughput	Specify performance in terms of throughput. Throughput is the measure of the amount of work performed by a software system over a period of time and can be expressed in terms of completing a specified quantity of an object over a period of time.	Throughput	1
19	Reliability	Specify the extent to which the software can perform its critical functions without failure for a specified period of time under specified conditions. This is typically expressed in terms of number of failures over a period of time.	Reliability specification	1

4.4.2. Failure Modes

Technical Evaluation				
#	*CCFAs*	*Description*	*Acceptance Criteria*	*Method of Verification*
20	Abnormal Behavior: Response to Abnormal Conditions and Events	Unintended inputs Software crash Software does not respond Unexpected output signal / result File corrupted or failed to be create Performance delay/failure	Actions to be performed when an abnormal condition or event occurs	1, 3, 4
21	System Environment Compatibility: Recovery	If required, the measure of the effort/time required to migrate the software to an equivalent hardware platform, component or environment.	Recovery time	1

ATTACHMENT 8.2
Commercial Grade Dedication Plan for Software
Page 17 of 27

4.4.3. Functionality Critical Characteristics

Technical Evaluation				
#	*CCFAs*	*Description*	*Acceptance Criteria*	*Method of Verification*
22	Functionality: Consistency with appropriate engineering/ scientific research and professional technical approaches	The degree in which the software's sample or complete data sets of results correlate with experimental data or professional analyses and any erroneous data sets do not correlate with the experimental data or professional analyses. (e.g., software output correlates with experimental data to +/- 3σ.)	If applicable, specify output correlation	1, 2, 4
23	Functionality: Correctness (correctness, proof of correctness)	Correctness may be expressed as how well the software satisfies its requirements and may be expressed as the maximum number of defects identified for each requirement. The severity or impact on performing the safety function correctly should be a factor in determining correctness. (e.g., 0 major defects reported, 5 minor defects reported, and 3 minor defects repaired and being tested.) Specify any formal techniques needed to mathematically prove that the software satisfies its specified requirements?	Correctness tests or proof(s).	1, 2
24	Functionality: Cyber security functions	Specify protections included in the software that eliminate or mitigate unwanted access or unintended modification of the software. (e.g. strong passwords, biometric access, firewalls, security of network.)	Specific cyber security requirements	1, 3
25	Functionality: Interface Communications (usability, interoperability, communicativeness)	Specify how the software accepts input from or can send output to other systems. Specify communication ports. Specify the ease in which operator controls are received by the software (e.g., all operator controls are via haptic devices such as joysticks).	Specify communication	1, 3
26	Functionality: Specific safety functions and algorithms	Specify the critical functions or calculations to be performed. Specify time-dependent functions to be performed.	Specify critical functions or calculation	1, 3, 4

ATTACHMENT 8.2
Commercial Grade Dedication Plan for Software
Page 18 of 27

4.5. Vendor Critical Characteristics

4.5.1. Service Conditions

Technical Evaluation				
#	***CCFAs***	***Description***	***Acceptance Criteria***	***Method of Verification***
27	Vendor support response	Requirement that the vendor respond within a period of time to support requests and errors.	Contractual requirement for response time	2
28	Ability to update software or firmware	Requirement that the software be able to be updated to perform corrective maintenance.	Post installation updates are possible	2
29	Problem Reporting: Notification to Customers	Notification by the vendor to customers of potential software defects or weaknesses. Notification to Customers criteria may be the presence and use of a problem reporting system, use of problem reporting metrics, and number of notifications to the users over time. Notification to Customers criteria verification is performed by reviewing communications of defects with users, review of any web site or other form of communicating with the vendor, and review of a log of communications.	Contractual requirement for error notification within a period of time	2
30	Supportability	The ability for the vendor to continue support for the software over the life of its use. This critical characteristic is important because of the difficulty to ensure the software is free of all defects. This critical characteristic should be considered when alternative software is not easily obtained or where financially not feasible. Supportability criteria can be the stability of the vendor based upon longevity of business (e.g. 20 years in business), size of customer base (e.g. 1000 customers world-wide), planned future product releases (e.g. vendor R&D has updates scheduled for next 3 years), and vendor history of discontinuing products (e.g., cancelled 3 product lines over past 2 years.	Contractual requirement for support. Review of the vendor history for the specific software as well as their history in supporting similar software or products.	2, 4

ATTACHMENT 8.2
Commercial Grade Dedication Plan for Software
Page 19 of 27

4.5.2. Qualifications

Technical Evaluation				
#	***CCFAs***	***Description***	***Acceptance Criteria***	***Method of Verification***
31	Training, knowledge and proficiency of personnel performing the work	Staff training, knowledge and proficiency criteria may include how well the specific staff member satisfies the vendor's qualification requirements for the position held. • Training in areas related to design or verification responsibilities • Experience in similar projects • Familiarity with specific tools, languages, etc., used in design The criteria can be quantified as the percentage of qualification requirements met, years of experience on similar projects, and/or certification level.	Evidence of attendance at courses, staff resumes, and on the job training against the vendor qualification requirements to determine how well the staff member satisfies the requirements.	2
32	Review of qualifications and experience of personnel involved in design and verification	Organization has experience in developing similar products. Third-party certifications as they relate to organizational capabilities	Evidence of developing similar products.	2

4.5.3. Operating History

Technical Evaluation				
#	***CCFAs***	***Description***	***Acceptance Criteria***	***Method of Verification***
33	Operating History	Documented: • Records indicating specific models and computer program(s)/firmware versions installed, when, and where • Formal or informal problem reports, description of problem and follow-up action Sufficient: • Number of units in service • Number of years of service Successful: • Error tracking shows good performance • Error rate has stabilized, no critical errors, computer program(s) stable other than feature changes Relevant: • Same or similar computer program(s)/hardware configuration, and functions or options used • Device installed and operated in a manner similar to the planned application • Similar environmental conditions • Similar run times	Documented, sufficient, successful and relevant operating history.	2, 4

ATTACHMENT 8.2
Commercial Grade Dedication Plan for Software
Page 20 of 27

4.6. Dependability / Built-in-Quality / SQA Program

For software-based systems, high quality is best achieved by: building it in, following a systematic life cycle approach from requirements through implementation, with verification and validation steps, and appropriate documentation for each phase of the life cycle.

The following a cross-reference between the software engineering phase, SRNS SQA Program and possible Critical Characteristics for Acceptance. The sub-sections below have additional example CCFAs.

Technical Evaluation			
SWE Phase	**SRNS Requirement (CCFA)**	**Acceptance Criteria**	***Method of Verification***
Software Quality Assurance Plan	SQAP	Existence of a QA Program Effective SQA Process SQA compliance for software being evaluated	1, 2, 3
Requirements	RSS	Evidence of a Requirements Specification for Software, or similar. Evidence of the intended-use of the software. Evidence that the software had safety as a requirement. Evidence of independent review of Requirements.	1
Requirements Traceability	RTM	Evidence that there is a link between requirements and specific test cases. Evidence of independent review of RTM or similar.	1
Design	DDS	Evidence that the software was designed using a software engineering process. Review of the design, its documentation, and hardware	2
IR	IR	Independent review of requirements and design documents	2, 3
Implementation and Testing	SW Test Cases and Results	Evidence that module-level testing was performed. / Testability Evidence that test results are maintained. / Defect Minimization/Tracking Evidence of regression testing. / Thoroughness of SW Testing Evidence of independent review of test cases and results.	1, 2
Safety Testing	Testing abnormal conditions/events and credible failures	Evidence of testing for abnormal conditions/events and credible failures.	1, 2
Source Code Control	Source Code Configuration Control	Evidence of source code revision control.	1, 2
Configuration/ Version Control	Configuration Control	Existence of major software versions. Existence of minor software versions. Evidence of configuration control/ product baselining.	1, 2
Instruction Manual	Instruction Manual	Existence and evaluation of instruction manual.	1
Maintenance	Maintenance	Evidence of corrective maintenance.	2, 3
Retirement	Retirement	Evidence of a method to retire the software.	1

ATTACHMENT 8.2
Commercial Grade Dedication Plan for Software
Page 21 of 27

4.6.1. SQA Program

Technical Evaluation				
#	*CCFAs*	*Description*	*Acceptance Criteria*	*Method of Verification*
34	Existence of QA Program	A QA program that includes documented procedures or process controls exists.	One or more of: • Vendor program certifications (e.g., ISO 9000, European certifications). • A QA program that includes documented procedures or process controls. • QA Program generally complies with a recognized standard (e.g. ISO 9000, ASME NQA-1). • Appropriate internal or external audit reports. • Performance of a survey against the chosen recognized standard.	1, 2
35	Effective SQA Process	A measure of how well the process meets its purpose and objectives. This critical characteristic can be used to provide an indicator of the defects remaining in the software. Process effectiveness criteria can be based upon the degree in which 3rd party certification/recertification programs are achieved (e.g., 90% of achievement of compliance to CMMI SEI maturity level 4 or achieved ISO 9000) or by qualitative measures of conformance to the vendor procedures (e.g., 75% of vendor software procedures are met).	Inspection of the proof of 3rd party certification. Review of vendor procedures and objective evidence that processes performed to produce the software is complaint with those procedures.	1, 2
36	SQA compliance for software being evaluated	Was an SQA process followed for the item being dedicated?	Application of SQA program to item being procured: • How strictly the program was adhered to for this product, degree of buy-in by personnel involved • How well documented, how formal, approvals required • Software life cycle is specified and used for product development, verification and validation	3

ATTACHMENT 8.2
Commercial Grade Dedication Plan for Software
Page 22 of 27

4.6.2. Requirements Traceability

Technical Evaluation				
#	*CCFAs*	*Description*	*Acceptance Criteria*	*Method of Verification*
37	Requirements Traceability	Traceability from system requirements and design through software requirements, software design, code, and validation testing.	Evidence of traceability from system requirements and design through software requirements, software design, implementation, and testing. Evidence of independent review of RTM or similar.	1

4.6.3. Design

Technical Evaluation				
#	*CCFAs*	*Description*	*Acceptance Criteria*	*Method of Verification*
38	Evidence that the software was designed using a software engineering process.	Documented evidence that the software was designed prior to implementation to meet critical requirements.	Evidence that the software was designed using a software engineering process. Evidence of independent review of Design.	1
39	Review of the design, its documentation, and hardware	Documentation of software design. Good design can be characterized by one or more: • Completeness • Accuracy and consistency with actual design • Overall system design and software architecture: • Simplicity • Determinism of program execution, control flow and data flow • Internal consistency • Adequacy to support needed functionality • Unneeded features and their impact to the required functionality • Error handling capabilities, built-in protective features, ability to handle expected and unforeseen errors and ACEs • Human factors and the HMI Protection against EMI-induced and other errors	Evidence of good design	1

ATTACHMENT 8.2
Commercial Grade Dedication Plan for Software
Page 23 of 27

4.6.4. Design for Reliability

Technical Evaluation				
#	*CCFAs*	*Description*	*Acceptance Criteria*	*Method of Verification*
40	Design for Reliability: Isolation	The software design implements methods of cohesion, reduces coupling, and promotes modularity. Cohesion is a module or routine that performs a single task or function. Modularity or decoupling is a module or routine that performs an independent task or function. Nominally, this is a qualitative measure. This critical characteristic provides an indicator to determine how much of the non-safety portions of the software must be included in the CGD process to provide the reasonable assurance that the failure of non-safety functions will not impact the proper execution of the safety functions. Isolation of safety functions criteria can be the total number of software modules that perform safety and non-safety functions, there is no sharing of logic between safety and non-safety modules, and non-safety modules or routines may only read output of safety modules or routines.	Evidence of isolation of safety critical function	2
41	Design for Reliability: Redundancy	The software design to implement duplication of critical components with the intention of increasing reliability. This critical characteristic may be important when the failure of the safety function can lead to severe consequences that harm the individuals or the environment. This critical characteristic may be more applicable to software that controls instrumentation. Redundancy criteria may include the existence of back-up critical hardware computing systems, multiple software development teams, information redundancy, multiple controllers, and dual processors.	Evidence of redundancy	2

ATTACHMENT 8.2
Commercial Grade Dedication Plan for Software
Page 24 of 27

4.6.5. Independent Review

Technical Evaluation				
#	*CCFAs*	*Description*	*Acceptance Criteria*	*Method of Verification*
42	Independent review of requirements and design documents	Adequacy of software/hardware requirements: • Completeness • Correctness • Clarity Design reviews and verifications: • Extent and coverage of reviews and analyses (design reviews, code walkthroughs and inspections, use of analytical tools) Independence of reviewers and verifiers Criteria for internal reviews and verifications effectiveness may include the ratio of defects identified during the review/verification and the number of defects that are discovered in the next life cycle phase. (e.g., ratio of the number of requirements defects identified during requirements review and the number of defects detected during the design phase).	Evidence of requirements reviews. Evidence of design reviews. Reviewed by an independent and qualified reviewer. Requirements and design documents are reviewed by an independent and qualified reviewer	2, 3

4.6.6. Implementation

Technical Evaluation				
#	*CCFAs*	*Description*	*Acceptance Criteria*	*Method of Verification*
43	Adherence to coding practices	The degree to which the software complies with the approved coding standards, use of code libraries, or automated configuration management tool. Examples of quality coding practices, include: • Documented coding standards. • Use of code libraries. • Use of integrated development tools that provide error checking. • Use of static analysis tools for source code. • Effort to reduce code complexity. • Documented code and function/module interfaces.	Evidence of quality coding practices. Evidence of source-code version management tools. Review of code inspection reports or other vendor evidence that included reviews of coding practice for the subject code modules.	2

ATTACHMENT 8.2
Commercial Grade Dedication Plan for Software
Page 25 of 27

4.6.6. Implementation, (cont.)

44	Defect Minimization	The degree to which defects are minimized. Indicators include defect density, effectiveness of defect detection techniques to keep defects from entering the next software life cycle phase, and severity of the defects detected. This critical characteristic can be used to provide an indicator of the defects remaining in the software. Defect minimization criteria may be the number of defects detected per lines of code, number of defects per pre- and post-release, and number of defects per software lifecycle phase.	Evidence of defect tracking and resolution. Evidence of defect minimization.	2

4.6.7. Testing

Technical Evaluation				
#	***CCFAs***	***Description***	***Acceptance Criteria***	***Method of Verification***
45	Testability	The measure of the effort required to perform software verification, validation, and installation testing. This critical characteristic may be appropriate to use when assurance is needed that reviews and tests were adequately performed. Testability criteria are based on the ease or difficulty in conducting verification and validation activities. Testability metrics may include: # of hours to perform peer reviews, # of hours to pretest a module, and # of hours to develop test cases.	Evidence of specific tests for specific requirements and/or evidence of testability metrics. Evidence of module-level testing and regression testing.	1
46	Thoroughness of software testing	A measure of the completeness of the software testing to ensure that the software is correct and complete. This critical characteristic may be appropriate to use for ensuring that tests were adequate to provide the reasonable assurance that the safety functions can be performed satisfactorily. Metrics can include: • Quantity of defects discovered during the various testing activities (pre- and post-release defects) • Percentage of source code covered by test cases • Percentage of lines, branches, modules, and functions tested • Successful performance and functional testing • Percentage of critical-characteristics that are covered by specific test cases	Evidence of traceability of safety requirements to tests completed. Evidence that the code was thoroughly tested (e.g. code coverage, module testing, range testing of parameters).	2
47	Independent review of test cases and results	For the software being evaluated, were the test cases and their results reviewed and approved by a qualified reviewer?	Evidence that test cases and their results were conducted and approved by a qualified reviewer.	2

ATTACHMENT 8.2
Commercial Grade Dedication Plan for Software
Page 26 of 27

4.6.8. Configuration Control

Technical Evaluation				
#	*CCFAs*	*Description*	*Acceptance Criteria*	*Method of Verification*
48	Configuration Control: Control of enhancements	The software improvements are controlled, approved, and necessary. Requirements churn is minimized but not zero. This critical characteristic may be appropriate to use when the stability of the software is important. This critical characteristic can provide an indicator as to the number of defects inserted into the software during the change process. Statistics may include number of enhancements (e.g., 15 changes/last year), and number of approved enhancements (e.g., 7 changes/last year), and number of completed enhancements (e.g., 3 changes/last year).	Control of enhancements criteria can be obtained from configuration control board statistics. Review of meeting minutes of a configuration control board, data from change logs and release notes.	2
49	Review of vendor configuration control program and practices	Application of configuration management program to item being procured: • How strictly the program was adhered to for this product • How well documented, from initial development through changes and releases • Control over sub-vendors • Control over distributors or suppliers through which the procured items pass	Documented configuration management program that is consistent with relevant standards and accepted practices (e.g., IEEE) Vendor program certifications (e.g., ISO 9000, European certifications) Vendor and product track record for control of changes and versions, and notification of changes, especially in repair.	1

4.6.9. Instruction Manual

Technical Evaluation				
#	*CCFAs*	*Description*	*Acceptance Criteria*	*Method of Verification*
50	Instruction Manual	Instructions for properly using the software. This can be in the form of a printed or electronic guide.	Existence of an instruction manual.	1, 2

Note: Nothing is specified about Instruction Manuals by *DOE Guidance For Commercial Grade Dedication*, April 2011 Draft

ATTACHMENT 8.2
Commercial Grade Dedication Plan for Software
Page 27 of 27

4.6.10. Maintenance

Technical Evaluation				
#	*CCFAs*	*Description*	*Acceptance Criteria*	*Method of Verification*
51	Maintainability	The software design that provides for ease in performing modifications to the software. This critical characteristic may be more appropriate for software whose failure could result in few or no alternatives should the software be unusable. Review of vendor metrics associated with the length of time to evaluate the change/defect correction, make the code change/correction, test the change/correction, update all software documentation, and release the change. Maintainability criteria can be based upon the time required to change the software. This criterion can be expressed as mean time to change or mean time to fix.	Evidence of corrective maintenance and regression testing.	2
52	Total Quality Management	Systematic application of lessons learned from problems experienced with earlier versions of the product	Evidence of application of lessons-learned from prior errors	2, 3

4.6.11. Retirement

Technical Evaluation				
#	*CCFAs*	*Description*	*Acceptance Criteria*	*Method of Verification*
53	Retirement	Notification from vendor that the software is no longer being actively supported and/or has been retired.	Requirement that the vendor notify customer that the software is no longer being supported.	1

Note: Nothing on retirement is specified by *DOE Guidance for Commercial Grade Dedication*, April 2011 Draft